



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Takanori MASUI et al.

Application No.: 10/653,216

Filed: September 3, 2003

Docket No.: 116970

For: DATA SECURITY IN AN INFORMATION PROCESSING DEVICE

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-081558 filed March 24, 2003

In support of this claim, a certified copy of said original foreign application:

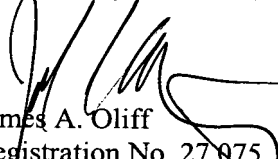
 X is filed herewith.

 was filed on in Parent Application No. filed .

 will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,


James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/al

Date: October 3, 2003

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 2 4 日
Date of Application:

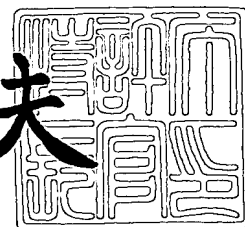
出 願 番 号 特 願 2 0 0 3 - 0 8 1 5 5 8
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 8 1 5 5 8]

出 願 人 富士ゼロックス株式会社
Applicant(s):

2 0 0 3 年 9 月 1 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 FE03-00217

【提出日】 平成15年 3月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

【氏名】 益井 隆徳

【発明者】

【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

【氏名】 横濱 竜彦

【発明者】

【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

【氏名】 佐竹 雅紀

【特許出願人】

【識別番号】 000005496

【氏名又は名称】 富士ゼロックス株式会社

【代理人】

【識別番号】 100075258

【弁理士】

【氏名又は名称】 吉田 研二

【電話番号】 0422-21-2340

【選任した代理人】**【識別番号】** 100096976**【弁理士】****【氏名又は名称】** 石田 純**【電話番号】** 0422-21-2340**【手数料の表示】****【予納台帳番号】** 001753**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 情報処理装置

【特許請求の範囲】

【請求項 1】 暗号化されたデータを入力する入力部と、
前記入力部により入力されたデータを、該データを暗号化した暗号鍵の対となる復号鍵を用いて復号化する復号処理部と、
前記復号処理部により復号化されたデータを、前記暗号鍵とは異なる暗号鍵を用いて暗号化する暗号処理部と、
前記暗号処理部により暗号化されたデータを記憶する記憶部と
を備えることを特徴とする情報処理装置。

【請求項 2】 請求項 1 記載の情報処理装置であって、
前記暗号処理部により暗号化処理を行なう際に用いられる暗号鍵には、有効期限が設定されていないことを特徴とする情報処理装置。

【請求項 3】 請求項 1 記載の情報処理装置であって、
前記入力部は、暗号化されていないデータも入力し、
前記暗号処理部は、前記入力部により入力された暗号化されていないデータも暗号化する
ことを特徴とする情報処理装置。

【請求項 4】 請求項 1 記載の情報処理装置であって、
前記暗号処理部により暗号化処理を行なう際に用いられる暗号鍵を生成する鍵生成部を備えることを特徴とする情報処理装置。

【請求項 5】 請求項 4 記載の情報処理装置であって、
揮発性メモリと、
前記鍵生成部により生成された暗号鍵を前記揮発性メモリに記憶させる記憶制御部と、
を備えることを特徴とする情報処理装置。

【請求項 6】 請求項 4 に記載の情報処理装置であって、
前記鍵生成部は、自装置固有の情報を用いて暗号鍵を生成することを特徴とする情報処理装置。

【請求項 7】 請求項 4 に記載の情報処理装置であって、
前記鍵生成部は、自装置の電源が投入されたことを契機として暗号鍵を生成することを特徴とする情報処理装置。

【請求項 8】 請求項 4 に記載の情報処理装置であって、
鍵生成パラメータを記憶した可搬型記憶媒体を着脱自在に装着可能な装着部を更に備え、
前記鍵生成部は、前記鍵生成パラメータから前記暗号鍵を生成するものである、
情報処理装置。

【請求項 9】 請求項 4 に記載の情報処理装置であって、
当該情報処理装置のセキュリティレベルの設定を行なうセキュリティ設定部を更に備え、
前記鍵生成部は、前記セキュリティ設定部で設定されたセキュリティレベルに応じた鍵長の暗号鍵を作成することを特徴とする情報処理装置。

【請求項 10】 請求項 4 に記載の情報処理装置であって、
自装置が使用される地域の設定を受け付ける地域設定部を更に備え、
前記鍵生成部は、前記地域設定部で設定された地域に応じた鍵長の前記暗号鍵を作成することを特徴とする情報処理装置。

【請求項 11】 請求項 1 に記載の情報処理装置であって、
前記暗号鍵を記憶した可搬型記憶媒体を着脱自在に装着可能な装着部を更に備え、
前記暗号処理部は、該装着部に装着された可搬型記憶媒体から前記暗号鍵を読み出して暗号化を行うことを特徴とする情報処理装置。

【請求項 12】 請求項 1 に記載の情報処理装置であって、
前記記憶部を複数備え、
前記暗号鍵を前記記憶部毎に対応させて有し、

前記暗号処理部は、データの保管先に決定された記憶部に対応する暗号鍵で暗号化することを特徴とする情報処理装置。

【請求項 13】 請求項 1 記載の情報処理装置であって、
前記暗号鍵を自装置を使用するユーザ毎に対応させて有し、
前記暗号処理部は、前記データに対応するユーザの暗号鍵で暗号化することを特徴とする情報処理装置。

【請求項 14】 請求項 1 記載の情報処理装置であって、
前記入力部により入力されたデータを暗号化するか否かを決定する決定手段と

、
前記決定手段により暗号化すると決定されたデータについて、前記暗号処理部により暗号化することを特徴とする情報処理装置。

【請求項 15】 請求項 14 記載の情報処理装置であって、
前記決定手段は、入力部により入力されたデータが暗号化されている場合は、暗号化すると決定することを特徴とする情報処理装置。

【請求項 16】 請求項 1 記載の情報処理装置であって、
記憶部により記憶されたデータを復号化してプリントするプリント部を備えることを特徴とする情報処理装置。

【請求項 17】 暗号化されたデータを入力し、
入力されたデータを、該データを暗号化した暗号鍵の対となる復号鍵を用いて復号化し、
復号化されたデータを、前記暗号鍵とは異なる暗号鍵を用いて暗号化し、
暗号化されたデータを記憶する
ことを特徴とする情報処理方法。

【請求項 18】 コンピュータに、
暗号化されたデータを入力する手順と、
入力されたデータを、該データを暗号化した暗号鍵の対となる復号鍵を用いて復号化する手順と、
復号化されたデータを、前記暗号鍵とは異なる暗号鍵を用いて暗号化する手順と、

暗号化されたデータを記憶する手順とを
実行させることを特徴とするプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ネットワークを介して受信した処理指示データや処理対象データに従って処理を実行する情報処理装置に関し、特にそれらデータのセキュリティのための技術に関する。

【 0 0 0 2 】

【従来の技術】

近年、ネットワーク化やこれに伴う情報犯罪の増加を背景として、情報セキュリティ強化への要望が高まっている。この要望に応えるものとして、公開鍵暗号方式を用いた P K I（公開鍵基盤）という基盤技術が広まりつつあり、コピー機や複合機、ファクシミリなどの情報機器にも P K I 対応のものが各種開発されている。

【 0 0 0 3 】

P K I 対応機器は、外部の P C（パーソナルコンピュータ）や各種装置から、ネットワークを介して、自装置の公開鍵で暗号化された処理指示データや処理対象データを受信する。この場合、P K I 対応機器が受信した暗号化データに対して行う処理の形態は、次の 2 つに大別できる。

【 0 0 0 4 】

まず第 1 は、受信した暗号化データを自機器の秘密鍵で復号し、その復号結果に基づき即座に処理を実行するというものである。第 2 は、受信した暗号化データを自機器の秘密鍵で復号し、その復号結果をいったん当該機器内の記憶装置（例えばハードディスク）に保管し、保管したデータを後で取り出して処理を行うというものである。この第 2 の処理形態の例としては、例えば親展プリントがある。親展プリント処理では、プリンタは、ユーザが外部 P C から送信してきた印刷データを内にいったん保存し、ユーザが自機器に対して正しいパスワードを入力したことを条件として、その保存した印刷データの印刷処理を実行する。

【0 0 0 5】

また、従来の、受信した暗号化データを復号して処理する画像処理装置としては、特許文献 1 に示されるものが知られている。

【0 0 0 6】

【特許文献 1】

特開平 0 9 - 1 3 4 2 6 4 号公報

【0 0 0 7】

【発明が解決しようとする課題】

このように、従来の P K I 対応機器では、上記第 2 の形態の処理を行う場合、該機器内の記憶装置にデータが復号された状態で長期間保管される可能性があるため、その間に情報漏洩の脅威がある。

【0 0 0 8】

これに対する対策としては、上記第 2 の形態の処理の場合には、復号したデータの代わりに、外部装置から受け取った暗号化データを記憶装置に保管しておく方法が考えられる。しかしながら、この方法には次のような問題がある。

【0 0 0 9】

まず第 1 に、P K I では認証局（C A）が公開鍵を証明した公開鍵証明書を信頼の基盤としているが、この公開鍵証明書には有効期限（通常 1 年）があり、この有効期限が切れると新たに別の秘密鍵・公開鍵のペアを生成して公開鍵証明書の交付を受ける。このため、古い公開鍵で暗号化されたデータが機器内の記憶装置に保管されている場合、そのデータに対する処理を実行するには、現在有効な秘密鍵だけでなく、古い秘密鍵も保存しておかなければならない。機器が、公的な認証局や、社内 C A のプライベートな認証局など、複数の認証局が発行した公開鍵証明書を用いる場合は、古い秘密鍵の管理が煩雑になる。この問題は、プリンタや複合機等におけるプリント処理といった短期的に記憶すればよいデータについて顕著である。すなわち、このようなデータは、長期的に保存されることが少ないにも係わらず、その少ないデータのために秘密鍵の履歴管理が必要となってしまう。

【0 0 1 0】

第2に、機器に対して外部装置から送信されてくる暗号化データの暗号強度は、その外部装置が用いた暗号方式や鍵長に依存する。このため、異なる外部装置からの暗号化データは、それぞれ暗号強度が異なることがある。その一方、企業内の情報セキュリティ管理では、企業内の機器に保存されるデータの暗号強度を一定以上に保ちたいという要請がある。外部装置から受け取った暗号化データをそのまま保管したのでは、この要件を満足できない。

【0011】

【課題を解決するための手段】

本発明に係る情報処理装置は、暗号化されたデータを入力する入力部と、前記入力部により入力されたデータを、該データを暗号化した暗号鍵の対となる復号鍵を用いて復号化する復号処理部と、前記復号処理部により復号化されたデータを、前記暗号鍵とは異なる暗号鍵を用いて暗号化する暗号処理部と、前記暗号処理部により暗号化されたデータを記憶する記憶部と、を備える。

【0012】

本発明の好適な態様では、前記暗号処理部により暗号化処理を行なう際に用いられる暗号鍵を生成する鍵生成部を有する。

【0013】

更に好適な態様では、揮発性メモリと、前記鍵生成部により生成された暗号鍵を前記揮発性メモリに記憶させる記憶制御部と、を備える。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。以下では、本発明に係る情報処理装置の一例として、デジタル複合機などの画像形成装置の例を説明する。

【0015】

まず、図1を参照して、本実施形態の画像形成装置のハードウェア構成を説明する。図1は、本実施形態の制御の説明のために必要な構成要素を図示したものであり、その他の構成要素については図示を省略している。

【0016】

この画像形成装置は、デジタル複写機やデジタル複合機など、原稿を光学的に読み取って得た画像をデジタルデータとして取り扱うタイプの装置である。この画像形成装置は、PKI対応の機能を備えている。すなわち、この画像形成装置は、認証局から自らに交付された公開鍵証明書に対応する秘密鍵・公開鍵のペアを有し、その公開鍵を用いて暗号化された外部装置からのデータをその秘密鍵を用いて復号する機能を備える。また、この画像形成装置は、外部装置に対してデータを送信する場合、そのデータをその外部装置の公開鍵を用いて暗号化する機能を備える。

【0017】

この装置においてROM（リード・オンリ・メモリ）12には、この画像形成装置の動作制御のための制御プログラムなどのデジタル情報が格納されている。CPU（中央処理装置）10がこのROM12内の制御プログラムを実行することにより、画像形成装置の各部の制御が実現される。PKI対応処理の機能や、後述する保管データに対する秘密保護の機能を記述したプログラムも、このROM12に格納されている。

【0018】

RAM（ランダム・アクセス・メモリ）14は、この画像形成装置の主記憶装置であり、制御プログラムの実行の際にワークメモリとしても用いられる。RAM14は、例えば、プリントエンジン28に供給する1ページ分の画像データを蓄えるページバッファとして用いることもできる。

【0019】

HDD（ハードディスク・ドライブ）16は、各種のデータを保存するための補助記憶装置である。例えば、HDD16には、画像形成装置が、要求される各種ジョブのために受信したり生成したりしたジョブデータが保存される。このようなジョブデータとしては、例えば、リモートホストからネットワークを介して依頼された印刷ジョブの印刷対象文書データ、コピーのためにスキャンエンジン26で読み取った原稿画像データや、スキャン指示に従ってスキャンエンジン26で読み取った画像データなどがある。

【0020】

不揮発性メモリ 18 (NVM: Non-Volatile Memory) は、この画像形成装置の制御に関する各種の半永久的な設定情報やプログラムを記憶するためのメモリであり、例えばEEPROMなどから構成される。なお、画像形成装置には、HDD 16 がオプションとなっている機種も多い。そのような機種では、HDD 16 が装備されない場合、ジョブデータがこのNVM 18 に記憶されることになる。

【0021】

なお、この画像形成装置に対して交付された公開鍵証明書に対応する秘密鍵は、上記HDD 16 又はNVM 18 のどちらかに保管される。

【0022】

ワンタイムPROM (one-time Programmable Read Only Memory) 20 は、1 回のみ書き込みが可能な不揮発性メモリである。このワンタイムPROMには、例えば画像形成装置の一意的な装置シリアル番号が記録される。

【0023】

操作パネル 22 は、この画像形成装置のユーザインタフェースのための表示や、ユーザからの各種指示の入力受付などのためのユーザインタフェース手段である。操作パネル 22 は、典型的には、コピースタートボタンなどの機械的な操作ボタンや液晶タッチパネルを備える。液晶タッチパネルは、CPU 10 で実行される制御プログラムが生成したGUI (グラフィカルユーザインタフェース) 画面を表示し、そのディスプレイに対するユーザのタッチ位置を検出して制御プログラムに渡す。制御プログラムは、そのタッチ位置の情報からユーザの入力内容を解釈する。

【0024】

通信インタフェース 24 は、ローカルエリアネットワークなどのネットワークとのデータ通信のための制御を行う装置である。リモートホストからのプリント指示等は、この通信インタフェース 24 を介して画像形成装置内に入力される。

【0025】

スキャンエンジン 26 は、原稿を光学的に読み取って電子的な画像データを生成するスキャナ機能を提供する装置である。自動原稿送り装置 (ADF) (図示

省略) にセットされた原稿は、A D F の機能により 1 枚ずつスキャンエンジンに送られ、光学的に読み取られる。

【 0 0 2 6 】

プリントエンジン 2 8 は、C P U 1 0 の制御により供給される画像データを用紙に画像形成 (印刷) するプリンタ機能を提供する装置である。

【 0 0 2 7 】

トークン読取部 3 0 は、ユーザが保持するハードウェアトークンを受け入れ、このトークン内に記憶されたデータを読み取る装置である。ハードウェアトークンは、例えば I C カードや、U S B (Universal Serial Bus) 等の各種有線インタフェース規格に対応したデバイス、或いはBluetooth等の各種無線インタフェース規格に対応したデバイスなどとして構成される。

【 0 0 2 8 】

このような画像形成装置において、本実施形態では、H D D 1 6 等に保管するデータのセキュリティ向上を図る。

【 0 0 2 9 】

次に、図 2 を参照して、この画像形成装置の制御機構の主要部を説明する。

【 0 0 3 0 】

まず、データ受信部 5 0 は、L A N 等のデータ通信ネットワークに接続されており、そのネットワーク上の外部装置 (P C など) からジョブ要求を受信する。このジョブ要求には、要求する処理内容を示す指示データが含まれる。また、要求するジョブが印刷の場合は、印刷の対象となる文書データが含まれる。外部装置は、指示データやジョブの対象となる文書データを当該画像形成装置の公開鍵を用いて暗号化してから送信してくる場合がある。

【 0 0 3 1 】

ジョブ制御部 5 1 は、操作パネル 2 2 に表示されるユーザインタフェース画面を用いて入力されるジョブ要求や、通信インタフェース 2 4 及びデータ受信部 5 0 の機能により受信されるジョブ要求を受け付け、それら要求に係るジョブの実行を制御する。ジョブ制御部 5 1 は、入力されたジョブを待ち行列に登録し、そのジョブの実行順序が来た時に、アプリケーション 6 0 に必要なデータを与えて

ジョブを実行させる。また、ジョブ制御部 51 は、受信したデータが暗号化されている場合は、P K I 暗号処理部 52 に対してその復号を要求する。また、ジョブ制御部 51 は、実行するジョブが、ジョブデータの保管が必要なジョブである場合、そのデータを H D D 16 に保管するための処理を実行する。なお、ジョブデータの保管が必要なジョブには、親展プリントのジョブや、読み取った画像を親展ボックスに一時保管するジョブなどがある。親展プリントについては既に説明した。

【0032】

また、ジョブ制御部 51 は、いったん H D D 16 に保管したジョブデータをジョブ実行のために使用する時が来た場合には、それを読み出してアプリケーション 60 に与える。

【0033】

アプリケーション 60 は、ジョブ実行のために画像形成装置が提供する印刷機能、スキャン機能、ファクシミリ機能などの各種機能をする機能モジュールである。

【0034】

P K I 暗号処理部 52 は、公開鍵基盤に従った公開鍵暗号方式の暗号化及び復号処理、電子署名の付与及び検証の処理を実行する機能モジュールである。

【0035】

P K I 鍵管理部 54 は、P K I 暗号処理部 52 の暗号化及び復号、電子署名付与及び検証の処理に用いられる鍵情報を管理する機能モジュールである。P K I 鍵管理部 54 は、H D D 16 又は N V M 18 に記憶された当該画像形成装置の秘密鍵や公開鍵、外部装置の公開鍵を読み出す機能を備える。これらの鍵は、例えば、システム管理者がマニュアル作業で P K I 鍵管理部 54 に登録する。また、P K I 鍵管理部 54 が必要に応じて認証局からそれらの鍵を取得する構成としても良い。なお、認証局が発行する公開鍵証明書には有効期限があり、当該画像形成装置の公開鍵・秘密鍵はその有効期限が切れると、P K I のシステムでは事実上使用できない。

【0036】

内部鍵暗号処理部 5 6 は、H D D 1 6 に保管するデータに対する暗号化処理と、保管した暗号化データの復号処理を行う機能モジュールである。内部鍵暗号処理部 5 6 は、内部鍵を用いて暗号化及び復号の処理を行う。有効期限のある公開鍵や秘密鍵とは異なり、この内部鍵は無期限であり、画像形成装置のユーザが変更するまで、同じものを使用する。この暗号化及び復号には、ユーザのセキュリティに対する要求を満足できる暗号アルゴリズムであればどのような暗号アルゴリズムを用いても良い。使用するアルゴリズムにより、暗号化用と復号用の内部鍵が同一である共通鍵の場合もあれば、暗号化用と復号用とに別々の内部鍵を用いる非対称鍵の場合もある。

【 0 0 3 7 】

内部鍵管理部 5 8 は、内部鍵暗号処理部 5 6 の暗号化及び復号処理に用いる内部鍵の情報を管理する機能モジュールである。

【 0 0 3 8 】

好適な実施例では、内部鍵管理部 5 8 は、内部鍵を、当該画像形成装置固有の情報に基づき自動生成する。一つの例としては、ワンタイム P R O M 2 0 に記憶された装置シリアル番号から内部鍵を生成する方法がある。内部鍵を生成するための鍵生成プログラムは、R O M 1 2 に記憶されている。内部鍵管理部 5 8 は、この鍵生成プログラムに対して装置シリアル番号をパラメータとして与えることで、内部鍵を生成する。鍵生成プログラムも装置シリアル番号も固定なので、この方法によれば、常に同じ値の内部鍵を生成することができる。内部鍵の生成は、暗号化や復号の必要が生じた時にその都度行うことも可能だが、所定のタイミングで内部鍵を生成し、それを R A M 1 4 に記憶して再利用することが好適である。この内部鍵生成のタイミングは、電源投入による画像形成装置の起動処理時が好適である。

【 0 0 3 9 】

この内部鍵の生成手順の一例を図 3 を用いて説明する。この処理は、起動時などに実行される。

【 0 0 4 0 】

この処理では、まず内部鍵管理部 5 8 は、ワンタイム P R O M 2 0 から装置シ

リアル番号を読み出す（S10）。次に、この装置シリアル番号をパラメータとして鍵生成プログラムを実行し、内部鍵の値を計算する（S12）。そして、このようにして計算した内部鍵の値をRAM14に記憶し、その内部鍵へのアクセス情報（例えばRAM14上での内部鍵のアドレス情報）を内部鍵暗号処理部56に通知する（S14）。内部鍵暗号処理部56は、暗号化や復号が必要になった場合、そのアクセス情報に基づき内部鍵の値を取得する。

【0041】

この例では、内部鍵そのものを画像形成装置の不揮発性の記憶媒体（HDD16やNVM18など）に記憶しないので、内部鍵の漏洩のリスクを低減できる。仮に装置シリアル番号が分かっても、鍵生成プログラムの秘密が保たれていれば、第三者が内部鍵を生成することはできない。また、この例では、生成された暗号鍵は揮発性のRAM14に記憶されるので、画像形成装置の電源を遮断したときに内部鍵は消える。これにより内部鍵のセキュリティを向上できる。

【0042】

次に、図4を参照して、この画像形成装置が、ネットワークを介して外部装置からジョブ要求のデータを受信した時の処理を説明する。

【0043】

この処理では、まずジョブ制御部51が、データ受信部50で受信されたデータが暗号化されているか否かを判定する（S20）。ここで、暗号化されていると判定した場合は、そのデータをPKI暗号処理部52に復号させる。これによりPKI暗号処理部52はPKI鍵管理部54から当該画像形成装置の秘密鍵を取得し、その秘密鍵を用いてデータを復号する（S22）。

【0044】

この復号処理の例を、図5に示す暗号化データの例を利用して説明する。

【0045】

図5に示す暗号化データは、W3Cの勧告案であるXML Encryptionに従ったものである。この例において、暗号化データ要素100には、データの暗号化に用いたアルゴリズムを示す要素102がまず記述される。要素102は、暗号化アルゴリズムとしてトリプルDESが用いられていることを示して

いる。

【 0 0 4 6 】

この次に、その暗号化アルゴリズムに用いた共通鍵を示す要素 1 1 0 及び 1 0 4 が記述されている。この例では、対象データを暗号化する際の共通鍵を、データ送信先である当該画像形成装置の公開鍵で暗号化している。要素 1 1 0 はこの暗号化された共通鍵の情報を記述する要素である。この要素 1 1 0 中には、共通鍵の暗号化に用いたアルゴリズムを示す要素 1 1 2 と、その暗号化に用いた鍵を示す要素 1 1 4 と、暗号化された共通鍵の値を示す要素 1 1 6 とが含まれる。暗号化鍵を示す要素 1 1 4 は、当該画像形成装置の名前を示している。これは、この名前に対応する公開鍵が用いられていることを意味する。

【 0 0 4 7 】

この要素 1 1 0 の後続く要素 1 0 4 は、データに対する暗号化のための鍵としてその要素 1 1 0 に示される鍵を用いることを示す参照情報を含む。

【 0 0 4 8 】

そして、このような鍵情報を示す要素 1 1 0 及び 1 0 4 の後に、データの暗号化結果の値を示す要素 1 0 6 が記述される。

【 0 0 4 9 】

このような暗号化データを受け取った P K I 暗号処理部 5 2 は、まず要素 1 1 6 に示された暗号化共通鍵の値を、当該画像形成装置の秘密鍵を用いて復号する。次に、要素 1 0 6 に含まれる暗号化されたデータ値を、要素 1 0 2 に示されたアルゴリズムとその共通鍵を用いて復号することで、平文のデータを復元する。

【 0 0 5 0 】

再び図 4 の処理手順の説明に戻る。ジョブ制御部 5 1 は、受信したデータが保管を要するものか否かを判定する（S 2 4）。この判定は、受信したデータに対応する指示データに示されるジョブの種別に基づき行うことができる。例えば、外部装置が要求したジョブの種別が、親展プリントのようにジョブ処理をすぐには実行しないタイプであれば、保管が必要と判定する。これに対し、通常のプリントジョブのように、すぐにジョブ処理を実行するタイプのジョブは、データの保管が不要と判定される。外部装置からの指示データが暗号化されている場合は

、このステップ S 2 4 の判定処理は、その指示データの復号の後に実行されることになる。

【0051】

ステップ S 2 4 の判定で、データの保管が不要と判定した場合は、ジョブ制御部 5 1 は、P K I 暗号処理部 5 2 で復号されたデータに対する処理を、できるだけ速やかに実行する（S 2 6）。

【0052】

これに対し、データの保管が必要と判定された場合は、更に保管するデータに対する秘密保護が必要か否かを判定する（S 2 8）。この判定は、そのデータ（あるいはそのデータを対象とするジョブ）の属性情報に基づき行うことができる。この判定に用いることができる属性としては、そのデータに対してジョブ要求者が指定した機密度や保管時間などを挙げることができる。ここで、保管時間は、ジョブ要求者が画像形成装置に当該データを保管してほしい期間の長さを示す。この画像形成装置は、そのデータを受信してから保管時間が経過すると、そのデータを破棄する。なお保管時間の代わりに保管期限の時刻を用いても良い。この例では、外部装置に設けられるプリンタドライバのユーザインタフェースにより、ユーザから、親展プリントのための認証情報（例えばパスフレーズ）、機密度、及び保管時間の入力を受け付ける。プリンタドライバは、入力されたそれら各情報を指示データに組み込んで、この画像形成装置に送信する。

【0053】

ステップ S 2 8 における判定処理の一例を図 6 に示す。この例では、ジョブ制御部 5 1 は、そのジョブの指示データに示された機密度と保管時間を、それぞれ対応するしきい値（このしきい値はあらかじめ当該画像形成装置の管理者が設定しておく）と比較し（S 4 0 及び S 4 2）、いずれか一方がしきい値より大きい場合、秘密保護が必要と判定する（S 4 4）。一方、機密度も保管時間もしきい値以下であれば、秘密保護が不要と判定する（S 4 6）。

【0054】

図 6 の例では、データ保護の必要性を判定するのに、ユーザが指定した機密度や保管時間を用いたが、これは一例に過ぎない。この代わりに例えば、受信した

暗号化データの暗号化に用いられた共通鍵（図5の要素116）の鍵長に基づきそのデータの機密度を判定し、その機密度に応じて秘密保護の要否を判定してもよい。

【0055】

またこの判定の更に別の例として、当該画像形成装置に入力されたデータが暗号化されている場合は、そのデータの保管する場合に秘密保護が必要であると判定する、という判定方式もある。これは、データを暗号化して当該画像形成装置に送ってくる以上、送り手側がデータの秘密保護を欲していると想定し、その意図に沿って保管の際には暗号化を行おうというものである。なおこの方式では、入力されたデータが暗号化されていない場合については、単に保管時には暗号化不要と判定してもよいし、別の詳細な判定規則を定めてもよい。

【0056】

また、そのデータの保管先の記憶装置に応じて、秘密保護の要否を判定することもできる。すなわち、前述したように、HDD16がオプション装備である画像形成装置の場合、HDD16を備えない構成では、保管データは不揮発性メモリ18に保管されることになる。ここで、HDD16は画像形成装置本体からの取り外しが比較的容易なので、例えば不正利用者が夜間などに取り外して内容を解析する可能性がある。これに対し、不揮発性メモリ18は、画像形成装置の基板に固定されているので、取り外して解析される可能性は低い。オプションのHDD16が装備されているか否かは、機器構成情報の1つとして不揮発性メモリ18に記録される。したがって、秘密保護要否判定のプログラムは、その機器構成情報を参照してHDD16が装備されているか否かを調べ、装備されていれば保管するデータの秘密保護が必要と判定し、装備されていなければ秘密保護が不要と判定する。

【0057】

また、ジョブ要求者が、ジョブに対してデータの秘密保護の要否を指定できるようにしてもよい。この場合、ジョブの指示データに秘密保護の要否の情報が組み込まれ、画像形成装置に送られる。

【0058】

再び図4の処理手順の説明に戻ると、ステップS28にて、保管するデータの秘密保護が不要と判定した場合は、ジョブ制御部51は、PKI暗号処理部52によるデータ復号結果を暗号化せずにHDD16に格納する(S30)。これに対し、保管するデータの秘密保護が必要と判定された場合は、ジョブ制御部51は、PKI暗号処理部52によるデータ復号結果を内部鍵暗号処理部56に暗号化させ、その暗号化結果をHDD16に格納する(S32)。

【0059】

このようにして保管したデータについて、ジョブ処理を実行する時が来ると、ジョブ制御部51は、HDD16からその保管データを取り出し、このデータが暗号化されて入れば、内部鍵暗号処理部56によりこれを復号してから、アプリケーション60に供給する。

【0060】

以上、外部装置からネットワークを介して受信したデータを保管する際の処理について説明した。なお、本実施形態の画像形成装置では、このような受信データのみならず、スキャンエンジン26により生成された画像データなど、画像形成装置内で生成されたデータをHDD16に保管する際にも、そのデータを内部鍵暗号処理部56で暗号化することができる。

【0061】

以上説明したように本実施形態の画像形成装置では、外部装置から受信した公開鍵暗号化データを、いったん復号した後、自装置の内部鍵で再暗号化して保管する。公開鍵で暗号化された受信データそのものを保管する場合は、古い秘密鍵の管理が問題であったが、内部鍵は無期限の鍵なのでそのような問題は解消される。また、本実施形態では、内部鍵という統一した鍵で暗号化したデータを保管するので、HDD16内に保管される暗号化データの暗号強度は均一化される。内部鍵として用いる鍵の鍵長や内部鍵暗号処理部56の暗号アルゴリズムを適切に選択することで、HDD16内の保管データの暗号強度を一定以上に保ちたいという要求を満足させることができる。

【0062】

また仮に公開鍵で暗号化されたデータをそのままHDD16に保管する構成を

とった場合、保管していた秘密鍵が何らかの理由で破壊されてしまうと、その暗号化データが復号できなくなる危険があるが、本実施形態のように装置シリアル番号から生成した内部鍵で暗号化する構成では、そのような危険性を低減できる。すなわち、有効期限ごとに更新される秘密鍵はHDD16や不揮発性メモリ18に保管されるため、読み出しや書き込み動作が比較的多く、破壊のリスクがある程度あるが、装置シリアル番号が書き込まれるワンタイムPROM20や鍵生成プログラムが書き込まれたROM12はHDD16や不揮発性メモリ18に比べて破壊のリスクは少ない。

【0063】

以上に説明した実施の形態はあくまで一例に過ぎず、本発明の範囲内で様々な変形例が考えられる。

【0064】

例えば、内部鍵管理部58で生成する内部鍵を、ユーザが要求する暗号強度に応じたものとすることもできる。これには、ユーザが画像形成装置に対して、希望するセキュリティレベルの値を設定しておく。この設定値は、HDD16又は不揮発性メモリ18に保存される。内部鍵管理部58は、システム起動時などに、図7に示すように、装置シリアル番号(S10)の他にそのセキュリティレベルの設定値を読み出す(S11)。そして、セキュリティレベルに応じて内部鍵の鍵長を決定し、鍵生成アルゴリズムによりその鍵長の内部鍵を生成し(S12a)、RAM14に格納する(S14)。

【0065】

また、国によっては法律などにより暗号鍵の鍵長に制限が設けられる場合があるが、本実施形態の装置は、これに対応することもできる。例えば、画像形成装置のワンタイムPROM20又は不揮発性メモリ18には、その装置の出荷先の国を示す識別情報が書き込まれるので、内部鍵管理部58は、内部鍵生成処理時に、この出荷先国設定値を読み出し、この値に応じて内部鍵の鍵長を決定すればよい。

【0066】

また、上記実施形態では装置シリアル番号から内部鍵を生成しているが、画像

形成装置が備える記憶デバイスに保存された他の当該装置固有の情報から内部鍵を生成するようにしても良い。

【0 0 6 7】

また、装置シリアル番号に加え、ハードウェアトークン（以下トークンと略称）を援用して内部鍵を生成することも可能である。すなわち、この変形例では、装置シリアル番号に加え、トークンに記憶した情報を内部鍵生成のパラメータに用いる。トークンを援用することで、仮に内部鍵管理部 5 8 の鍵生成アルゴリズムが漏洩した場合でも、内部鍵を不正に生成することを困難にすることができる。

【0 0 6 8】

この方法での鍵生成処理の手順の一例を図 8 に示す。鍵生成を行う場合、内部鍵管理部 5 8 は、まず画像形成装置の鍵生成の設定が、トークンを用いる設定になっているか否かを判定する（S 5 0）。この設定は、画像形成装置の管理者が行い、その設定値が HDD 1 6 又は不揮発性メモリ 1 8 に保管されている。この判定で、トークンが不要と判定された場合は、図 3 に示した処理と同様の処理を実行する（S 1 0, S 1 2, S 1 4）。これに対し、鍵生成にトークンが必要と判定された場合、内部鍵管理部 5 8 は、トークン読取部 3 0 からトークンデータの入力があるか否かを判定する（S 5 2）。この入力がない場合は、操作パネル 2 2 のディスプレイに、トークンをセットすべき旨のエラーメッセージを表示し（S 5 4）、トークンのセットを促す。ステップ S 5 2 でトークンがセットされていると判定された場合は、内部鍵管理部 5 8 は、装置シリアル番号とそのトークンデータとそれぞれ読み出し（S 5 6）、それらをパラメータとして用いて内部鍵を生成し（S 5 8）、RAM 1 4 に記憶する（S 1 4）。

【0 0 6 9】

なお、装置シリアル番号を用いず、トークン内のパラメータのみを用いて内部鍵を生成する構成も考えられる。

【0 0 7 0】

また、内部鍵を画像形成装置内で生成する代わりに、トークン内に内部鍵を格納しておき、それを画像形成装置が読み出して利用する構成も可能である。

【 0 0 7 1 】

また、以上の例では、画像形成装置に対して1つの内部鍵を用いたが、画像形成装置に登録された登録ユーザごとに内部鍵を生成し、これを用いてユーザごとの暗号化を行うこともできる。この例では、画像形成装置は、受信した指示データや保管対象データのヘッダ情報などから、その保管対象データの所有者を判定し、PKI暗号処理部52の復号結果をその所有者の内部鍵を用いて再暗号化してHDD16に保管する。

【 0 0 7 2 】

以上、本発明をデジタル複合機等の画像形成装置に適用した場合の実施形態を説明した。しかしながら、上述の説明から明らかなように、本実施形態における格納データの秘密保護方式は、処理の種類や格納対象のデータの種類に依存しないので、画像形成装置以外の様々なジョブ処理装置に適用可能である。

【図面の簡単な説明】

【図1】 実施形態の画像形成装置のハードウェア構成の要部を示す図である。

【図2】 画像形成装置の制御機構の主要部を示す機能ブロック図である。

【図3】 内部鍵管理部による鍵生成手順の一例を示す図である。

【図4】 受信データに対する処理手順を示す図である。

【図5】 暗号化された受信データの一例を示す図である。

【図6】 保管データの暗号化の要否を判定する処理の手順の一例を示す図である。

【図7】 内部鍵管理部による鍵生成手順の別の例を示す図である。

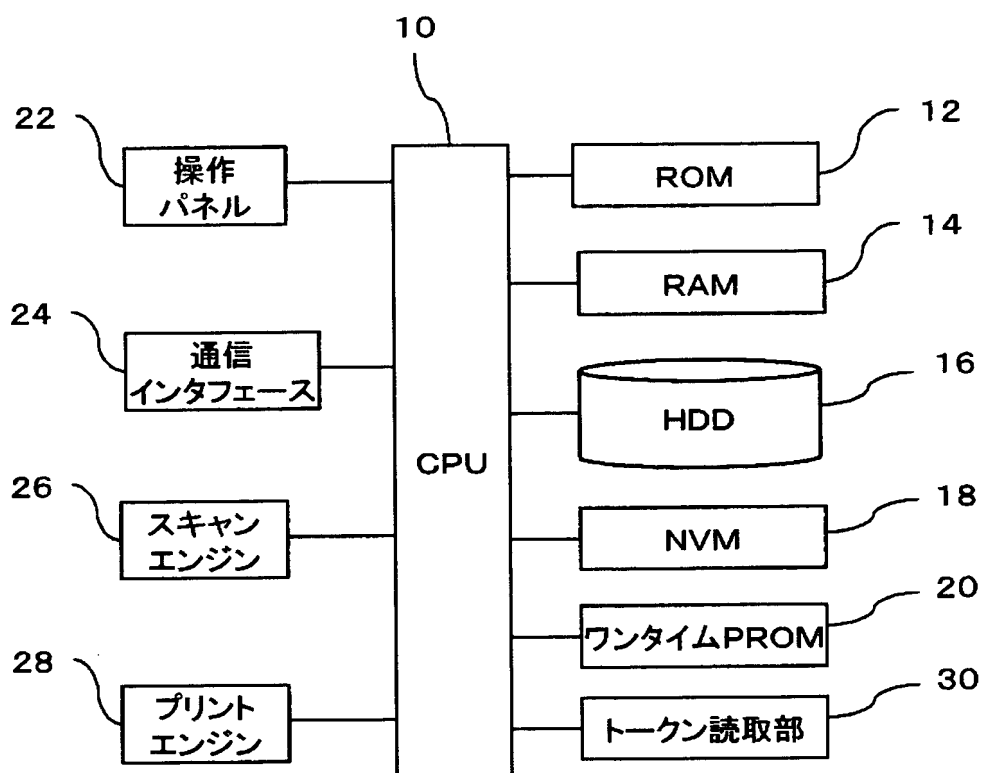
【図8】 内部鍵管理部による鍵生成手順の更に別の例を示す図である。

【符号の説明】

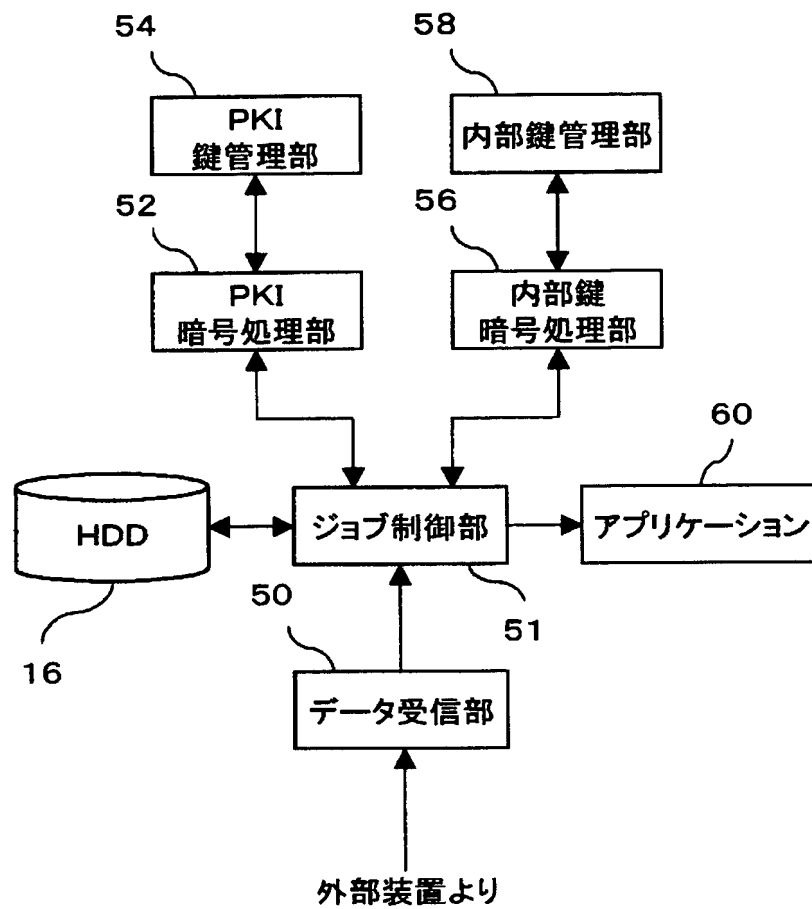
16 HDD（ハードディスク・ドライブ）、50 データ受信部、51 ジョブ制御部、52 PKI暗号処理部、54 PKI鍵管理部、56 内部鍵暗号処理部、58 内部鍵管理部、60 アプリケーション。

【書類名】 図面

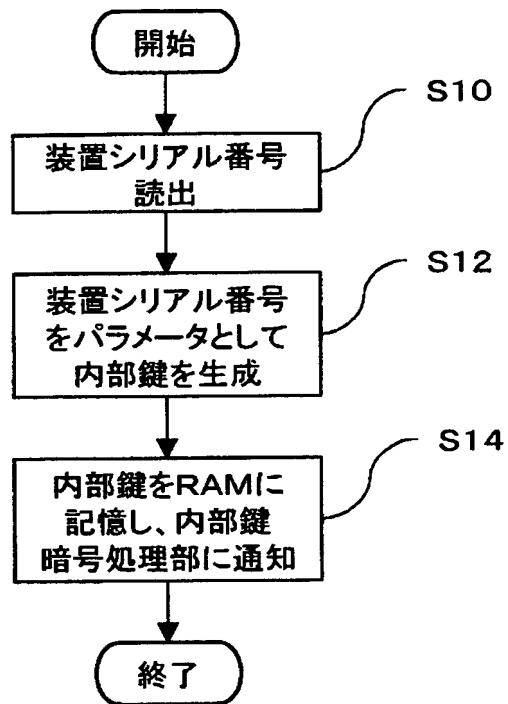
【図 1】



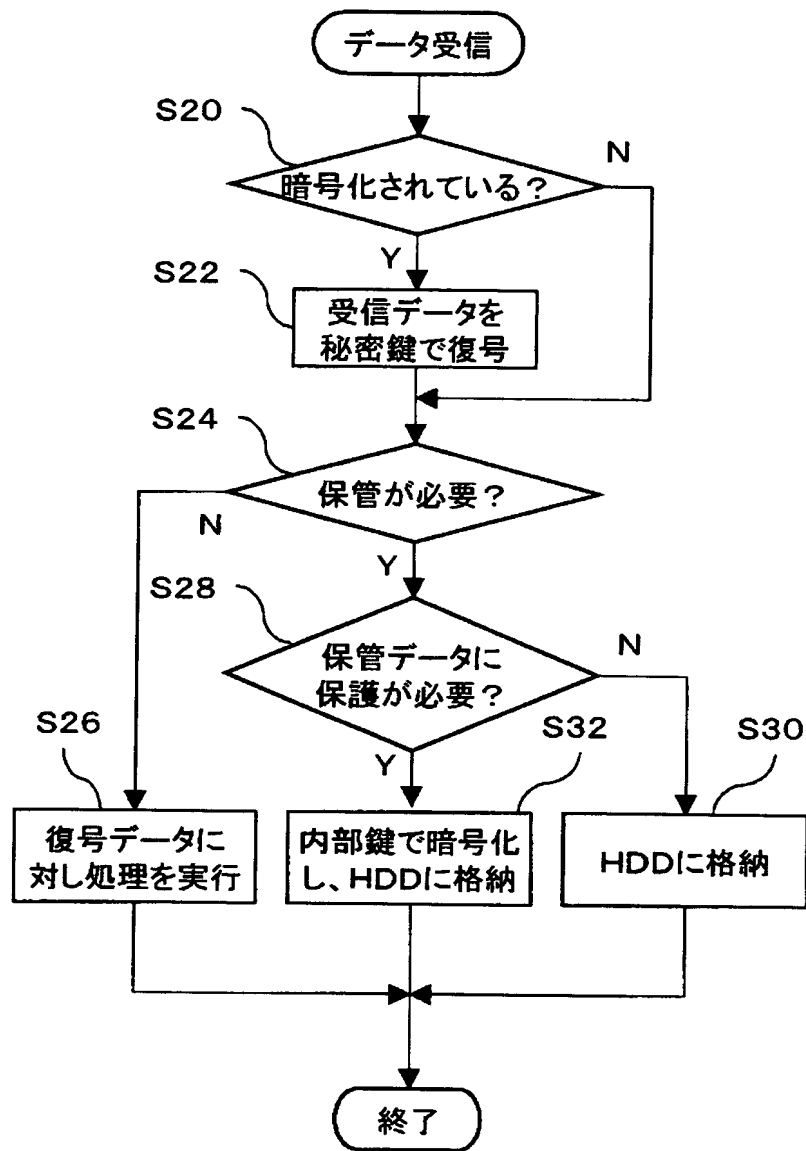
【図 2】



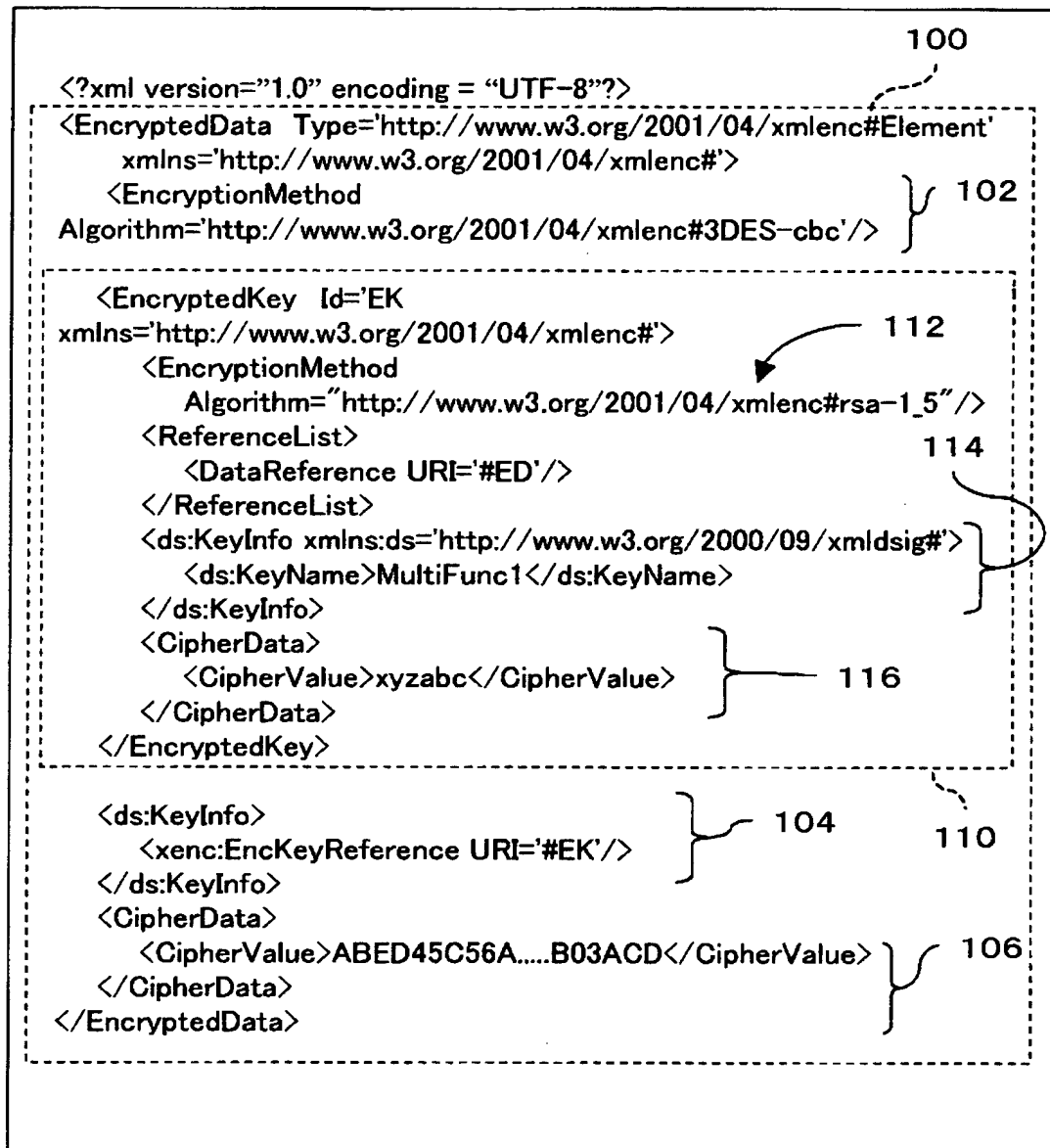
【図 3】



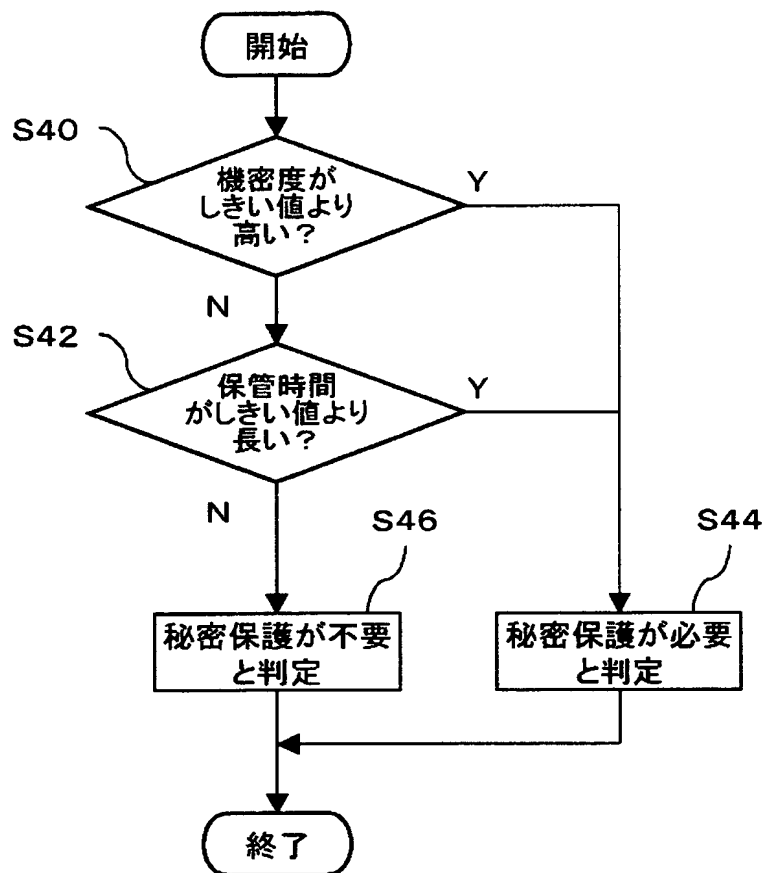
【図 4】



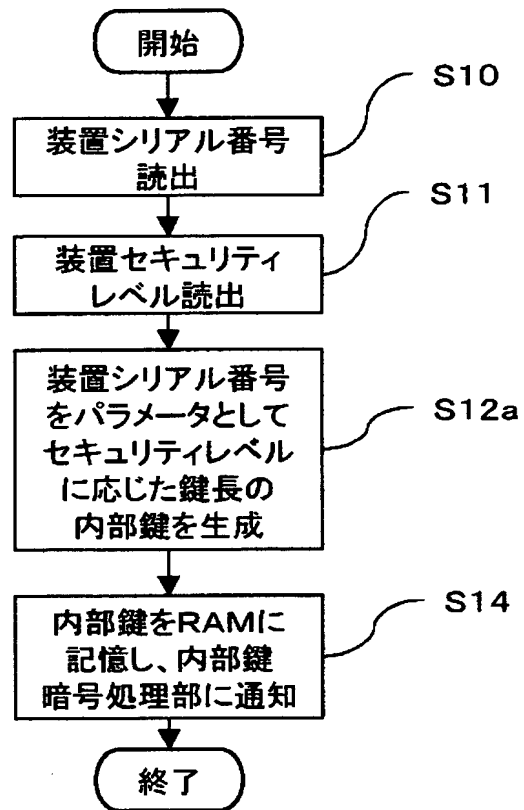
【図 5】



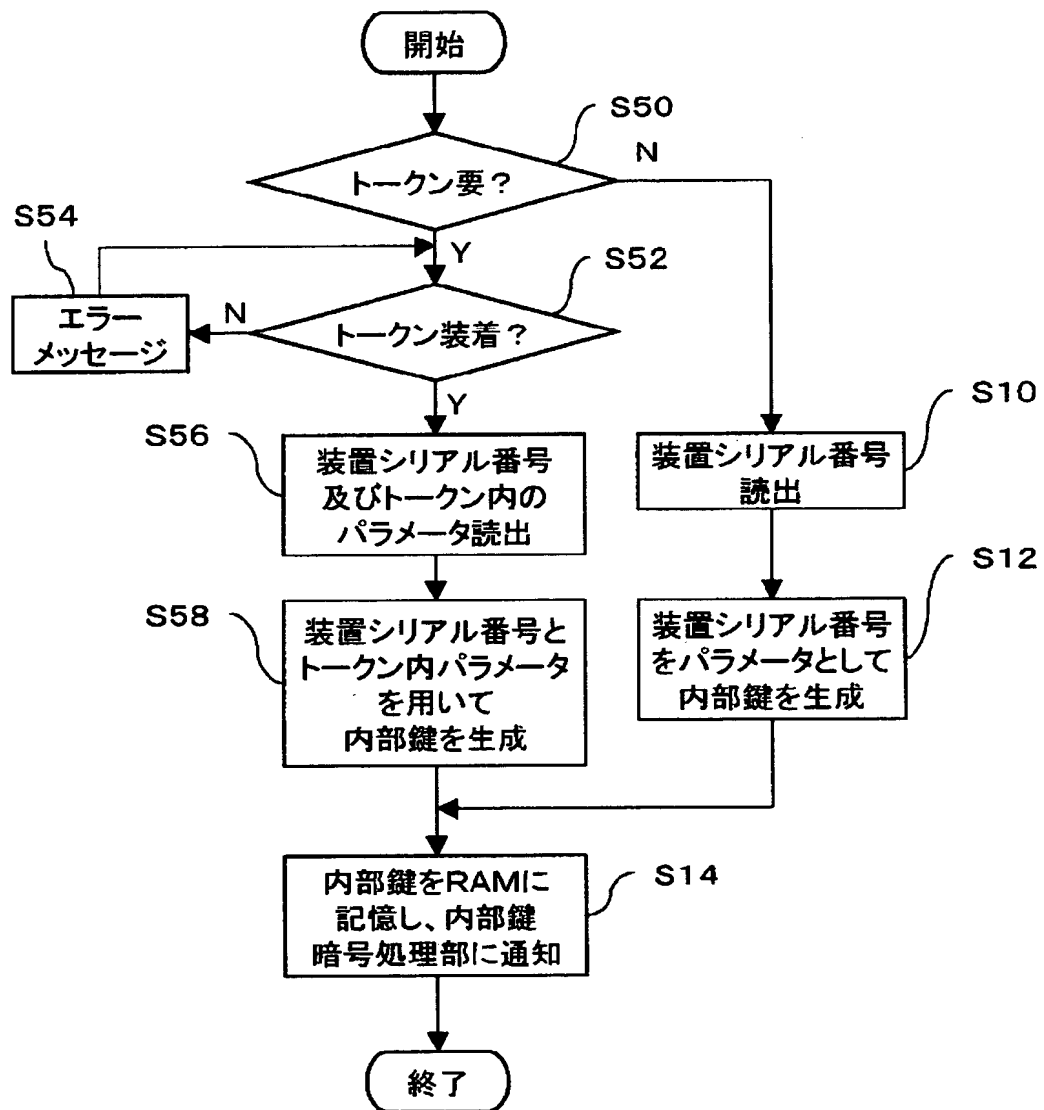
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 P K I（公開鍵基盤）のシステムにおいて、公開鍵で暗号化されたデータを受信して保管する場合の、保管データの秘密保護と使い勝手の両立を図る。

【解決手段】 データ受信部 5 0 で受信された公開鍵暗号化データは、P K I 暗号処理部 5 2 で秘密鍵を用いて復号される。ジョブ制御部 5 1 は、データに対する処理指示等に基づき、そのデータを秘密保護が必要か否かを判定する。秘密保護が必要な場合、そのデータを内部鍵暗号処理部 5 6 で暗号化した上で、H D D 1 6 に保管する。内部鍵暗号処理部 5 6 は、当該装置の装置シリアル番号から生成した内部鍵を用いてその暗号化を行う。内部鍵は、P K I の公開鍵と異なり有効期限がなく、更新の必要がないので、H D D 1 6 に保管された古いデータもその鍵で復号できる。

【選択図】 図 2

特 願 2 0 0 3 - 0 8 1 5 5 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 4 9 6]

1 . 変更年月日

1 9 9 6 年 5 月 2 9 日

[変更理由]

住所変更

住 所

東京都港区赤坂二丁目 1 7 番 2 2 号

氏 名

富士ゼロックス株式会社